RPLY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,726	01/14/2000	SHARON S. LIU	5437-106	8758

29989 7590 12/17/2003

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	9

DATE MAILED: 12/17/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/483,726	LIU ET AL.
	Examiner	Art Unit
	Paula W Klimach	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2, 5, and* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-6, 12-17, and 23-28 rejected under 35 U.S.C. 102(e) as being anticipated by Kumar et al (U.S Patent 6,535,980).

In reference to claims 1, 12, and 23, Kumar suggests a method, apparatus, and computer readable medium for verifying the legitimacy of an untrusted mechanism, comprising: submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism (column 3 lines 40-55); receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information (column 3 lines 56-67); determining whether each response received from the untrusted mechanism is a correct response (column 4 lines 5-8); and to in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate. The mechanism that is not legitimate will not get the correct key because the mechanism would not have the secret shared table (column 4 lines 15-21); and therefore would be determined to be illegitimate because it would not have the matching response that would result in the key.

2. Claims 2-6, 13-17, and 24-28 are rejected as the rejection in claims 1, 12 respectively above.

In reference to claims 2, 3, 13, 14, 24, and 25, wherein said sequence is generated randomly. The sequence is generated using a random number generator (column 4 lines 22-25).

In reference to claim 4, 15, and 26, wherein said sequence includes at least one submission of said first set of information and at least one submission of said second set of information (column 3 lines 54-55).

In reference to claims 5, 16, and 27, wherein said first set of information is designed to solicit a first proper response from the untrusted mechanism, and said second set of information is designed to solicit a second proper response from the untrusted mechanism, and wherein determining whether each response received from the untrusted mechanism is a correct response comprises: where the set of information submitted to the untrusted mechanism was said first set of information, determining whether the response from the untrusted mechanism is said first proper response (column 4 lines 6-7); and where the set of information submitted to the untrusted mechanism was said second set of information, determining whether the response from the untrusted mechanism is said second proper response (column 4 lines 9-11 in combination with column 3 lines 54-55).

In reference to claim 6, 17, and 28, wherein said first proper response is an affirmative response, and wherein said second proper response is a negative response (column 4 lines 7-8 in combination with column 3 lines 63-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 7-11, 18-22, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar in view of Shostack et al (U.S Patent 6,298,445 B1).

In reference to claims 7, 10-11, 18, 21-22, 29, and 32-33, Kumar suggests a method, apparatus, and computer readable medium for verifying the legitimacy of an untrusted mechanism, comprising: submitting a first information and second information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism, said first information being known to be verifiable, and said information being known to be unverifiable (column 3 lines 40-55); receiving a response from the untrusted mechanism for each submission of either said first information or said second information (column 3 lines 56-67); determining whether each response received from the untrusted mechanism is a correct response (column 4 lines 5-8); and in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate. Since the untrusted mechanism does not have the correct responses it cannot get the correct key and is therefore illegitimate.

Kumar does not expressly teach the information used for verification being a digital signature.

However, Shostack discloses the use of digital signatures to authenticate the integrity of the software enhancement (column 10 lines 21-24).

Regarding claims 10, 21, and 32, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature (Kumar column 3 lines 54-55). The reference Kumar discloses the use of at most k sets of information. Kumar does not expressly disclose the information to include digital signatures. Shostack discloses the use of digital certificates for authentication.

Regarding claims 11, 22, and 33 wherein determining whether each response received from the untrusted mechanism is a correct response comprises: where the signature submitted to the untrusted mechanism was said first signature, determining whether the response from the untrusted mechanism is that said first signature is verified (Kumar column 4 lines 6-7); and where the signature submitted to the untrusted mechanism was said second signature, determining whether the response from the untrusted mechanism is that said second signature is not verified (Kumar column 4 lines 9-11). Kumar does not expressly disclose the use of digital signatures as the challenge, however Shostack discloses the use of digital signatures for authentication. Therefore the signature submitted to the untrusted mechanism is similar to the signature disclosed by Shostack for authentication.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the digital signature as disclosed by Shostack in the system disclosed by Kumar. One of ordinary skill in the art would have been motivated to do this because the digital signature facilitates the authentication of the software by using a cryptographic function computed as a message and a user's private key. The signature function produces a value unique to the private key and the finger print value being signed. The private key has a mathematically related public key that anyone may use to verify the signature created by the private key (Shostack column 11 lines 10-17).

4. Claims 8-9, 19-20, and 30-31 are rejected as in the rejection for claims 7, 18, and 29 respectively above.

In reference to claims 8, 19, and 30, wherein said sequence is generated randomly (Kumar column 4 lines 22-25).

In reference to claims 9, 20, and 31, wherein said sequence is generated using a random number generator. It is inherent that a random sequence is generated using a random number generator.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
Wednesday, December 03, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100